## Remarks

Entry of this amendment, reconsideration of the application, and allowance of the claims as amended are respectfully requested. Claims 1, 2, 4, 5, 7-14, 16-19, 21-29, 31, 32 & 34-38 remain pending.

As requested, the specification has been amended to correct the misspellings of "thresholds" at page 8, line 28, and to clarify identification of the acronym "PES" as "packetized elementary stream" at page 18, lines 18-19. Based upon these amendments, withdrawal of the specification objections is requested.

Additionally, claims 1 & 14 have been amended to clarify that the "decryption unit" is part of the claimed invention. Further, claims 8, 24 & 35 are amended to characterize the stream of compressed data as comprising one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data. Further, claims 3, 11, 25 & 38 have been amended to specify that the encryption parameter comprises at least two of a number of parameter types. Based upon these amendments, withdrawal of the 35 U.S.C. §112 rejection to claims 1-26, 35 & 38 is requested.

By this amendment, independent claims 1, 14, 27 & 28 are amended to recite, in part, dynamically varying encrypting of the stream of data at the encryption unit by dynamically changing simultaneously multiple encryption parameters and signaling the dynamic change in encryption parameters to the encryption unit. The dynamic varying of the multiple encryption parameters is responsive to occurrence of a predefined condition in the stream of data. The characterization of dynamically changing simultaneously multiple encryption parameters is added to the independent claims to reinforce the clear departure of applicants' invention from the prior approaches, including those described in the applied art. Support for the claim amendments can be found throughout the application as filed. For example, reference the subject matter of canceled claims 3, 20 & 30 (which have been canceled herein without prejudice). No new matter is believed added to the application by any amendment presented.

Substantively, original claims 1, 2, 5-8, 12-19, 26 & 27 were rejected under 35 U.S.C. §102(b) as being anticipated by Jones (U.S. Patent No. 5,412,730), while claim 28 was rejected under 35 U.S.C. §102(b) as being anticipated by Warren et al. (U.S. Patent No. 5,719,937), and claims 1, 13, 14 & 26 were rejected under 35 U.S.C. §102(a) as being anticipated by Aucsmith et al. (U.S. Patent No. 5,991,403). Additionally, claims 3, 9-11, 20 and 22-25 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jones in view of Nardone et al. (U.S. Patent No. 5,805,700) and further in view of Leppek (U.S. Patent No. 5,933,501); claims 4 and 21 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jones in view of Nardone et al. and Leppek and further in view of "Digital Television Achieves Maturity" by Leonardo Chiariglione, copyrighted 1998 (herein referred to as "Chiariglione '98"); claims 29 and 32-35 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jones in view of Warren et al.; claims 30 and 36-38 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jones, Nardone et al., and Leppek in view of Warren et al.; and claim 31 was rejected under 35 U.S.C. §103(a) as being unpatentable over Jones, Nardone et al., Leppek, Chiariglione '98 in view of Warren et al. Each of these rejections is respectfully, but most strenuously, traversed to any extent deemed applicable to the amended claims submitted herewith.

Based upon the amendments submitted, all claim rejections are believed to be moot, with the possible exception of the rejection to claims 3, 9-11, 20 and 22-25 (as obvious over Jones, Nardone et al. and Leppek) since the subject matter of original claims 3 & 20 is now characterized by the corresponding amended independent claims. Thus, the comments which follow are principally addressed to an obviousness rejection to the independent claims based upon a purported combination of Jones, Nardone et al. and Leppek. Without addressing the combinability of these references, and assuming, arguendo, that the combination is proper, the combination still fails to teach or suggest features of applicants' invention recited in the independent claims presented herewith.

An "obviousness" determination requires an evaluation of whether the prior art taken as a whole would suggest the claimed invention taken as a whole to one of ordinary skill in the art. In evaluating claimed subject matter as a whole, the Federal Circuit has expressly mandated that functional claim language be considered in evaluating a claim relative to the

prior art. Applicants respectfully submit that the application of these standards to the independent claims presented herewith leads to the conclusion that the recited subject matter would not have been obvious to one of ordinary skill in the art based on the applied patents.

As recited in claim 1, for example, applicants' invention comprises a method for protecting a stream of data to be transferred between an encryption unit and a decryption unit. The method includes encrypting the stream of data at the encryption unit for transferring of the encrypted stream of data from the encryption unit to the decryption unit. The encrypting of the stream of data is dynamically varied at the encryption unit by dynamically changing simultaneously multiple encryption parameters of the encryption process, and signaling the dynamic change in encryption parameters to the decryption unit. The dynamically varying of the multiple encryption parameters is responsive to occurrence of a predefined condition in the stream of data. Upon receipt of the encrypted data at the decryption unit, the method includes decrypting the encrypted data, wherein the decrypting accounts for the dynamic varying of the encrypting by the encryption unit using the simultaneously changed, multiple encryption parameters.

Advantageously, the present invention provides a new technique for protecting a stream of data to be transferred between an encryption unit and a decryption unit. The technique includes dynamically changing simultaneously multiple encryption parameters used to encrypt the stream of data as the stream of data is passing through the encryption unit. This dynamically changing can occur periodically over time, for example, several times a second, thereby allowing only a small segment of the stream of data to be decoded should the encryption parameters used to encrypt that segment of data be uncovered. This concept of dynamically changing simultaneously multiple encryption parameters as a stream of data is being encrypted is believed to comprise a unique approach from any of the applied art, which typically rely upon definition of a predefined policy for changing the encryption process.

Jones describes an encrypted data transmission system employing means for "randomly" altering the encryption keys. Pseudo-random number generators are employed at both the transmitting and receiving stations to supply identical sequences of encryption keys

to a transmitting encoder and receiving decoder. An initial random number seed value is made available to both stations. The random number generators are advanced at times determined by predetermined characteristics of the data being transmitted so that, after transmission has taken place, the common encryption key can be known only to the transmitting and receiving stations.

A careful reading of Jones fails to uncover any teaching, suggestion or implication of applicants' concept of encrypting a stream of data and during the encryption process dynamically varying encrypting of the stream of data by dynamically changing simultaneously multiple encryption parameters. The Jones encryption approach requires pseudo-random binary sequence generation, and requires seed and mask values arranged at the sender and the receiver. Further, a change in Jones to the encryption process involves changing only an encryption key. The change in the encryption key occurs only at a predefined interval arranged a priori between the sender and the receiver. Jones changes the encryption key only when the counted number of bits or words or "items" matches the arranged interval. The disadvantage of this approach is that synchronization is absolutely essential. Bytes lost during transmission throw off the encryption/decryption process without any chance of recovery. In contrast, applicants' invention of dynamically varying simultaneously multiple encryption parameters as the stream of data is being encrypted ensures that only a small segment of the encrypted data could be exposed or lost should the encryption parameters used to encrypt that segment become uncovered or lost, respectively.

In addition, applicants' recited process includes signaling the dynamic change in the encryption parameters from the encryption unit to the decryption unit. A careful reading of Jones fails to uncover any teaching, suggestion or implication that the single encryption key change is signaled to the decryption unit. Rather, the patent teaches otherwise by describing a process which relies upon an a priori agreed upon process. In Jones, the decryption unit knows in advance where the encryption key change is to occur. In contrast, applicants recite a truly dynamic varying of the encryption process wherein the dynamically changed encryption keys are forwarded from the encryption unit to the decryption unit.

To summarize, there are multiple differences between applicants' recited technique for protecting a stream of data and the teachings of the Jones patent. For example, Jones relies upon a fixed policy or fixed sequence for changing a single encryption parameter. In contrast, applicants' invention comprises dynamically changing the encryption process by simultaneously changing multiple encryption parameters as the stream of data is being encrypted. Because applicants' approach does not rely upon a predefined policy, the dynamic change in the encryption parameter is signaled from the encryption unit to the decryption unit.

Nardone et al. describe a policy based selective encryption of compressed video data. Basic transfer units of compressed video data of a video image are selectively encrypted in Nardone et al. in accordance with an encryption policy to degrade the video image to at least a virtually useless state, i.e., if the selectively encrypted compressed video image were to be rendered without decryption.

A careful reading of Nardone et al. fails to uncover any dynamic varying of the encryption parameters as a stream of data is being encrypted within an encryption unit as recited by applicants. The Office Action notes that Nardone et al. teach encrypting of a bit stream taking into account encryption granularity, density and delay. However, Nardone et al. do not describe dynamically varying multiple ones of these encryption parameters simultaneously as the encryption of a stream of data progresses.

Leppek describes a virtual encryption scheme which combines different encryption operators into a compound-encryption mechanism. The encryption operators in Leppek refer to different encryption processes. Thus, in Leppek, data is first encoded using a first encryption scheme, then the same data is encoded using a second encryption scheme, etc., thereby increasing the entropy of the data to make the encoded data look as random as possible.

In contrast, applicants recite dynamically changing simultaneously multiple encryption parameters while an encryption unit is encrypting a stream of data. In applicants' approach, different segments of the stream of data are encrypted using different encryption parameters and there is a dynamic change in the encryption parameters such that multiple

encryption parameters simultaneously change from one segment to another segment of the stream of data as the stream of data is passing through the encryption unit and being encrypted. In Leppek, there is a static, sequential application of a number of encryption algorithms or encryption operators to the same segment of data. Leppek describes encrypting the same data multiple times using different encryption operators (i.e., encryption schemes).

For all the above reasons, applicants respectfully request allowance of the independent claims presented herewith. The dependent claims are believed allowable for the same reasons as the independent claims from which they directly or ultimately depend, as well as for their own additional characterizations.

Neither Warren et al., Aucsmith et al., or Chiariglione '98 are believed to teach, suggest or imply the above-noted deficiencies of Jones, Nardone et al. and Leppek when applied against the independent claims presented herewith.

All pending claims are believed to be in condition for allowance and such action is respectfully requested. Should the Examiner wish to discuss this case with applicants' attorney, the Examiner is invited to contact applicants' representative at the below-listed number.

Respectfully submitted,

Kevin P. Radigan

Kevin P. Radigan
Attorney for Applicants
Registration No.: 31,789

Dated: December 23, 2003.

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 Columbia Circle
Albany, New York 12203-5160
Telephone: (518) 452-5600
Facsimile: (518) 452-5579